Listing of the Claims

1. (Currently amended) An apparatus comprising:

a tamper resistant digital content recovery module to recover protected digital content~~s~~ of various types in an obfuscated manner;

a plurality of plain text digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of the plain text digital content rendering modules~~which~~ to be selectively employed to render the recovered digital content~~s~~ of the various~~corresponding~~ types, including one of the plain text digital content rendering modules occupying a root position of the hierarchy to exclusively receive all types of the recovered digital content~~s~~ to be rendered, ~~of all types,~~ from the tamper resistant digital content recovery module;

one or more storage units operative to store said tamper resistant module and said plurality of plain text digital content rendering modules; and

a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules.

2. (Currently amended) The apparatus of claim 1, wherein the tamper resistant digital content recovery module is equipped to verify ~~to its satisfaction that~~ the plain text digital content rendering module occupying the root position of the hierarchy ~~h~~as not having been compromised, and to provide recovered digital content to the plain text digital content rendering module occupying the root position of the hierarchy, only upon having ~~so~~ verified ~~to its satisfaction that~~ the plain text digital content rendering module occupying the root position of the hierarchy ~~h~~as not having been compromised.

3. (Currently amended) The apparatus of claim 2, wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content

rendering module occupying the root position of the hierarchy, responsive to a request from the plain text digital content rendering module occupying the root position of the hierarchy to recover a protected digital content.

4. (Currently amended) The apparatus of claim 3, wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy by verifying a signature of the plain text digital content rendering module occupying the root position.

5. (Currently amended) The apparatus of claim 1, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and ~~each of at least a subset of~~ the non-leaf ~~plain text digital content rendering~~ module~~s~~ is equipped to verify ~~to its satisfaction that~~ the immediate downstream ~~plain text digital content rendering~~ module ~~or modules, if any, have~~ as not having been compromised.

6. (Currently amended) The apparatus of claim 5, wherein ~~each of the subset of~~ the non-leaf ~~plain text digital content rendering~~ module~~s~~ is equipped to verify ~~to satisfaction that~~ the immediate downstream ~~plain text digital content rendering~~ module ~~or modules~~ ~~ha~~s~~ve~~ not having been compromised, at least during initialization.

7. (Currently amended) The apparatus of claim 6, wherein ~~each of the subset of~~ the non-leaf ~~plain text digital content rendering~~ module~~s~~ is equipped to further verify ~~to its satisfaction that an~~the immediate downstream ~~plain text digital content rendering~~ module ~~or modules~~ remains un-compromised before each transfer of recovered digital content to the immediate downstream ~~plain text digital content rendering~~ module.

8. (Currently amended) The apparatus of claim 5, wherein ~~each of the subset of~~ the non-leaf ~~plain text digital content rendering~~ module~~s~~ is equipped to verify ~~to its satisfaction that~~ the immediate downstream ~~plain text digital content rendering~~ module ~~or modules have~~ as not having been compromised by verifying ~~corresponding~~ a signature ~~or signatures~~ of the immediate downstream ~~plain text digital content rendering~~ module ~~or modules~~.

9. (Currently amended) The apparatus of claim 1, wherein the digital content of various types comprise~~s~~ streaming media contents of a plurality of media, and of a plurality of format types.

10. (Currently amended) The apparatus of claim 1, wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, or~~and~~ a cluster of coupled systems.

11. (Original) The apparatus of claim 1, wherein a first subset of the plain text digital content rendering modules are member modules of a first application domain, and a second subset of the plain text digital content rendering modules are member modules of a second application domain.

12. (Currently amended) A processor implemented method, comprising:

a root one of a plurality of hierarchically organized plain text digital content rendering modules collectively ~~equipped~~ adapted to render digital content~~s~~ of a plurality of types;

requesting a tamper resistant digital content recovery module to recover a first protected digital content of a first type;

verifying with the tamper resistant digital content recovery module ~~verifying~~ that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been comprised;

recovering with the tamper resistant digital content recovery module ~~recovering~~ the first protected digital content in an obfuscated manner~~,~~;~~and~~

transferring the recovered first digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

rendering with said root one in conjunction with first at least one other one of said plurality of hierarchically organized plain text digital content rendering modules rendering said first digital content~~,~~; and

verifying with ~~each of~~ said root ~~and non-leaf~~ ones~~, if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules~~ ~~verifying~~ of the modules that one of the first at least one other one of the modules occupying an immediate downstream position in the hierarchy of modules from the root module, is uncompromised before transferring the first digital content to the verified immediate downstream module to further the rendering of the first digital content.

13. (Currently amended) The method of claim 12, wherein the tamper resistant module verifies the root one of the plurality of hierarchically organized plain text digital content rendering modules by verifying ~~its~~the root one's signature.

14. (Currently amended) The method of claim 12, wherein ~~each of~~ said root ~~and non-leaf~~ ones~~,~~ ~~if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules~~ verifies the~~an~~ one of the first one other one that

occupies an immediate downstream position in the hierarchy of modules from the root module is uncompromised by verifying the immediate downstream module's signature.

15. (Currently amended) The method of claim 12, wherein the method further comprises ~~each of~~ said root ~~and non-leaf~~ ones~~,~~ ~~if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules~~ verifies ~~its~~each module occupying an immediate downstream position in the hierarchy of modules from~~or~~ the root module~~s~~, ~~if any,~~ during initialization.

16. (Currently amended) The method of claim 12, wherein the method further comprises

the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of the same first type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been comprised;

the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with ~~each of~~ said root ~~and same non-leaf~~ ones~~,~~ ~~if any, of said first at least one other one of said plurality of hierarchically organized digital content rendering modules~~ re-verifying the~~an~~ same immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

17. (Currently amended) The method of claim 12, wherein the method further comprises

the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of a second type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been comprised;

the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with second at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with ~~each of~~ said root ~~and non-leaf~~ ones~~,~~ ~~if any, of said second at least one other one of said plurality of hierarchically organized digital content rendering modules~~ verifying one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

18. (Currently amended) An apparatus comprising:

a plurality of digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of ~~which~~ the modules to be selectively employed to protectively render digital content~~s~~ of various~~corresponding~~ types, including one of said digital content rendering modules occupying a root position of the hierarchy to exclusively receive ~~the~~ the various types of digital content~~s~~ to be rendered, ~~of all types,~~ from ~~at least~~ a ~~separate~~ recovery module not part of the hierarchy of modules, the recovery module being responsible for recovering the digital contents from their ciphered states, and ~~each of~~ the ~~non-leaf ones of the digital content rendering~~ root module~~s~~ being ~~responsible~~ operative for verifying ~~to its own satisfaction that its it's~~ a module occupying an immediate downstream position in the hierarchy of modules from~~or~~ the root module~~s, if any, have~~ as not having been compromised;

one or more storage units to store said plurality of digital content rendering modules; and

a processor coupled with the one or more storage units to execute the digital content rendering modules.

19. (Currently amended) The apparatus of claim 18, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and ~~each of~~ the non-leaf ~~ones of the digital content rendering~~ module~~s~~ is equipped to verify ~~to its satisfaction that~~ the immediate downstream module ~~or modules, if any, have~~ as not having been compromised, at least during initialization.

20. (Currently amended) The apparatus of claim 18, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and ~~each of~~ the non-leaf ~~ones of the digital content rendering~~ module~~s~~ is equipped to further verify to ~~its~~the ~~satisfaction that an~~ immediate downstream ~~digital~~

~~content rendering~~ module remains uncompromised before each transfer of digital contents to the immediate downstream digital content rendering module.

21. (Currently amended) The apparatus of claim 20, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and ~~each of~~ the non-leaf ~~ones of the digital content rendering~~ module~~s~~ is equipped to verify ~~to its satisfaction that~~ the immediate downstream ~~digital content rendering module or~~ module~~s, if any, have~~ as not having been compromised, by verifying ~~corresponding~~ a signature ~~or signatures~~ of the immediate downstream ~~digital content rendering module or~~ module~~s~~.

22. (Currently amended) The apparatus of claim 18, wherein the digital content of various types comprise~~s~~ streaming media contents of a plurality of media types, and of a plurality of format types.

23. (Currently amended) The apparatus of claim 18, wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, or~~and~~ a cluster of coupled systems.

24. (Currently amended) The apparatus of claim 18, wherein a first subset of the ~~non-leaf~~ modules are member modules of a first application domain, and a second subset of the ~~non-leaf~~ modules ~~modules~~ are member modules of a second application domain.

25. (Currently amended) A processor implemented method comprising:

verifying with ~~each~~ a root one of a plurality of hierarchically organized digital content rendering modules~~,~~ ~~verifying~~that ~~to its satisfaction that each of its~~ each module that occupies an immediate downstream position in the hierarchy of modules from the root module~~, if any, is~~ ~~as~~has not having been ~~un~~compromi~~z~~sed, during an initialization period;

exclusively receiving with the~~a~~ root one of the plurality of hierarchically organized digital content rendering modules ~~exclusively receiving~~ a first digital content of a first type; ~~and~~

rendering in part with said root one of said modules ~~in conjunction with first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering~~ said first digital content~~,~~;

re-verifying with ~~each of~~ said root ~~and non-leaf~~ ones of said modules that~~, if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules further~~ ~~verifying~~ one of the at least one other one of the modules occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised; and

~~before~~ transferring with said root one of said modules the first digital content to the re-verified immediate downstream module to further the rendering of the first digital content.

26. (Currently amended) The method of claim 25, wherein ~~each of~~ said root ~~and non-leaf~~ ones~~, if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules~~ verifies each~~an~~ immediate downstream module is uncompromised by verifying the immediate downstream module's signature.

27. (Currently amended) The method of claim 25, wherein the method further comprises

the root one of the plurality of hierarchically organized plain text digital content rendering modules receiving a second protected digital content of the same first type; and

said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with ~~each of~~ said root ~~and same non-leaf~~ ones~~,~~ ~~if any, of the first at least one other one of said plurality of hierarchically organized digital content rendering modules~~ re-verifying the same one of the first at least one other one ~~an~~ that occupies an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

28. (Currently amended) The method of claim 25, wherein the method further comprises

the root one of the plurality of hierarchically organized plain text digital content rendering modules receiving a second protected digital content of a second type; and

said root one in conjunction with second at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with ~~each of~~ said root ~~and non-leaf~~ ones~~,~~ ~~if any, of the second at least one other one of said plurality of hierarchically organized digital content rendering modules~~ re-verifying one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the re-verified one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module to further the rendering of the second digital content.

29. (Currently amended) An article of manufacture comprising:

a recordable medium;

a first plurality of programming instructions recorded on said recordable medium, ~~with~~ said first programming instructions ~~designed~~ adapted to program a computing device~~,~~ to implement on the computing device~~,~~ a tamper resistant digital content recovery module to recover protected digital content~~s~~ of various types in an obfuscated manner; and

a second plurality of programming instructions recorded on said recordable medium, ~~with~~ said second programming instructions ~~designed~~ operative to program the~~a~~ computing device~~,~~ to implement on the computing device~~,~~ a plurality of plain text digital content rendering modules, said rendering modules communicatively coupled with each other in a hierarchical manner ~~forming~~ to form a hierarchy of modules, ~~with selective combinations of~~ the plain text digital content rendering modules ~~which to be~~ being selectively employed in combination to render the recovered digital contents of the various~~corresponding~~ types~~,~~ including one of the plain text digital content rendering modules occupying a root position of the hierarchy to exclusively receive all types of the recovered digital contents to be rendered,~~ of all types,~~ from the~~a~~ tamper resistant digital content recovery module.

30. (Currently amended) The article of claim 29, wherein the tamper resistant digital content recovery module is equipped to verify ~~to its satisfaction that~~ the plain text digital content rendering module occupying the root position of the hierarchy has not been compromised, and to provide recovered digital content to the plain text digital content rendering module occupying the root position of the hierarchy, only upon having so verified ~~to its satisfaction~~ that the plain text digital content rendering module occupying the root position of the hierarchy has not been compromised.

31. (Currently amended) The article of claim 29, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and ~~each of at least a subset of the plain text digital content rendering~~the non-leaf module~~s~~ is equipped to verify ~~to its satisfaction that~~ the immediate downstream ~~plain text digital content rendering~~ module from the non-leaf module ~~or modules, if any, have~~ as not having been compromised.

32. (Currently amended) The article of claim 29, wherein the digital content of various types comprise~~s~~ streaming media contents of a plurality of media, and of a plurality of format types.

33. (Original) The article of claim 29, wherein the recordable medium is a selected one of a magnetically recordable medium and an optically recordable medium.